UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/039,429	01/02/2002	David Marshall Ross		2870

30914 7590 03/24/2005

DAVID M. ROSS
31 SEAL RIVER ROAD
ROSBURG, WA 98643

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/039,429	ROSS, DAVID MARSHALL	
	Examiner	Art Unit	
	Eleni A Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 1-6 are rejected under 35 U.S.C. 101 because the invention is directed to non-statutory subject matter. It is not tangibly embodied, as it is only process/software per se. It is suggested that the claimed subject matter "A process for ..." should be changed to "a process/program stored on a computer-readable medium...".

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 7 is rejected under 35 U.S.C. 102(e) as being anticipated by Shefi (Patent No.: US 6,445,794 B1).

As per claim 7 Shefi teaches the process for the secure transmission of information over a

medium, wherein a plurality of stations intercommunicate over said medium, where the cipher system used in said secure transmission process uses expendable data resources (52) which are diminished with use, and where one or more of said plurality of stations is an originator station (44) and has available to said originator station a source of truly random data (46), and where said originator station or said originator stations can employ a creation technique (50) to operate on truly random data (48) from said source of truly random data or said sources of truly random data and use said truly random data to create new versions of said expendable data resources, and where;

(d) said originator station or said originator stations can transmit to other said stations, as encrypted traffic over said medium, said new versions of said expendable data resources (Shefi Col. 18 lines 18-34, and lines 54-60);

whereby said process of secure transmission of information over said medium can continue and be regenerated depending on only the continued presence of said source of truly random data at said originator station or said originator stations (Shefi Col. 7 lines 60-67 and col. 5 lines 8-21);

and whereby any need for said expendable data resources coming from sources external to said plurality of stations is eliminated (Shefi Col. 18 lines 54-67).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shefi (Patent No.: US 6,445,794 B1) in view of Hattick et al. (Hattick, Pub. No.: US 2003/0112972 A1).

As per claim 1, Shefi teaches process for the secure transmission of information over a medium (36), using identical one time pads (28) which are present at a plurality of stations (22) which communicate over said medium, the process comprising the steps of:

(a) providing each said station with a pseudorandom number sequence generator (26) which can generate a pseudorandom number sequence (28) having properties and number sequence programmed (Shefi Col. 4 lines 65-col. 5 lines 7);

(c) allowing each of said plurality of stations to use said pseudorandom number sequence generator (Shefi Col. 4 lines 65-col. 5 lines 7) to generate said pseudorandom number sequence for use as said one time pad (Shefi Col. 18 lines 54-60);

(d) providing each said station with a mixing technique (30) wherein a plaintext message (34) can be encrypted by means of using said mixing technique to combine said plaintext message and said one time pad (Shefi Col. 16 lines 8-19);

thereby producing a ciphertext message (32) which can be securely transmitted over said medium (Shefi Fig. 2B step one-step three);

(e) providing each said station with an inverse mixing technique (42) wherein said ciphertext message can be decrypted by means of using said inverse mixing technique to combine said ciphertext message and said one time pad (Shefi Col. 16 lines 20-29);

thereby reproducing the original said plaintext message at any of said plurality of stations (Shefi Fig. 2B step four).

Shefi does not explicitly teach controlled by a replaceable element set (24) which defines and specifies said pseudorandom number sequence; and

(b) providing each said station with said replaceable element set, with all of said plurality of stations having identical said replaceable element sets;

However Hattick discloses a synchronizer to synchronize bits position in the one-time pad with the data carrier by moving to index i, or the ith bit of the onetime pad that reads on controlled by a replaceable element set (24) which defines and specifies said pseudorandom number sequence (Hattick page 3 par. 0024-25); and

(b) providing each said station with said replaceable element set, with all of said plurality of stations having identical said replaceable element sets (Hattick page 3 par. 0024-25);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Hattick within the system of Shefi because it would require generation and synchronization of the one-time pad in the reader to have a successful mutual authentication and data encryption/decryption (Hattick page 3 par. 0024) and would create multiple random number sequences from a single table of bits/replacement set by using different starting point.

As per claim 2, Shefi and Hattick teach all the subject matter as described above. In addition, the process, if said replaceable element set is shorter than said pseudorandom number sequence and said one time pad, it is useful to securely transmit said replaceable element set over said medium as an encrypted message (Hattick page. 3 par. 0024-0025),

allowing for the creation of multiple alternate pseudorandom number sequences at any of said stations (Shefi Col. 4 lines 65-col. 5 lines 7, col. 7 lines 60-67, and col. 5 lines 62-67), and

allowing the use of said multiple alternate pseudorandom number sequences as multiple alternate one time pads at any of said stations (Shefi Col. 4 lines 65-col. 5 lines 7, col. 7 lines 60-67, and col. 8 lines 16-22),

whereby any of said stations can receive said multiple alternate one time pads as encrypted traffic over said medium (Shefi Col. 17lines 42-56),

providing said stations with fresh and unique versions of said one time pads without the use of a separate and secure distribution path for said one time pads (Shefi Col. 5 lines 8-21). The rational for combining are the same as claim 1 above.

As per claim 3, Shefi and Hattick teach all the subject matter as described above. In addition, the process, since said replaceable element set is used with said pseudorandom number sequence generator to produce said pseudorandom number sequence and said one time pad,

and since alternate formats of said replaceable element sets (Hattick page 3 par. 0024) and said pseudorandom number sequence generators can be used (Shefi Col. 5 lines 8-39),

allowing the creation of multiple logical groups of said stations in which all said stations in each of said logical groups share at least one common said alternate format (Shefi Col. 4 lines 7-34),

whereby said logical groups can, by design, be allowed access or be denied access to other logical groups (Shefi Col. 18 lines 44-68). The rational for combining are the same as claim 1 above.

As per claim 4, Shefi and Hattick teach all the subject matter as described above. In addition, the process, since said replaceable element set is used with said pseudorandom number sequence generator to produce said pseudorandom number sequence (Hattick page 3 par. 0024),

and since the use of differing formats of replaceable element sets and differing formats of pseudorandom number sequence generators will produce pseudorandom number sequences having differing properties of randomness and unpredictability and sequence length (Hattick page 3 par. 0024),

the creation of pseudorandom number sequences having differing properties of randomness and unpredictability and sequence length is possible by varying the formats of said replaceable element sets and said pseudorandom number sequence generators (Shefi Col. 4 lines 65-col. 5 lines 7 and Hattick page 3 par. 0024). The rational for combining are the same as claim 1 above.

As per claim 5 Shefi and Hattick teach all the subject matter as described above. In addition,

Hattick teaches the process, since said replaceable element set is used with said pseudorandom number sequence generator to produce said pseudorandom number sequence,

and since the pseudorandom number sequence which is produced is a function of the starting point of the pseudorandom number sequence (Hattick page 3 par. 0024),

it is possible to create multiple pseudorandom number sequences from a single replaceable element set by using different starting points for each of said multiple pseudorandom number sequences (Hattick page 3 par. 0024 and page 5 lines 1-3). The rational for combining are the same as claim 1 above.

As per claim 6 Shefi and Hattick teach all the subject matter as described above. In addition, Hattick teaches the process, wherein said process of secure communication contains the step of sending along with the ciphertext message, a set of state information regarding the internal condition of said pseudorandom number sequence generator at the beginning of the encryption process of said ciphertext message (Hattick page 4 par. 0025). The rational for combining are the same as claim 1 above.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136
March 15, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100